(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/90987 A1

(51) International Patent Classification⁷: G06F 17/60

(21) International Application Number: PCT/SG01/00102

(22) International Filing Date: 25 May 2001 (25.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

PQ 7758	25 May 2000 (25.05.2000)	AU
PR 1598	21 November 2000 (21.11.2000)	AU

(71) Applicant and
(72) Inventor: GUEH, Wilson, How, Kiap [SG/SG]; Blk 347 Clementi Avenue 5, #05-66 Singapore 120347, Singapore 120347 (SG).

(74) Agent: SIM, Andrew, Yuan, Meng; Shook Lin & Bok, AIA Tower#18-00, 1 Robinson Road, Singapore 048542 (SG).

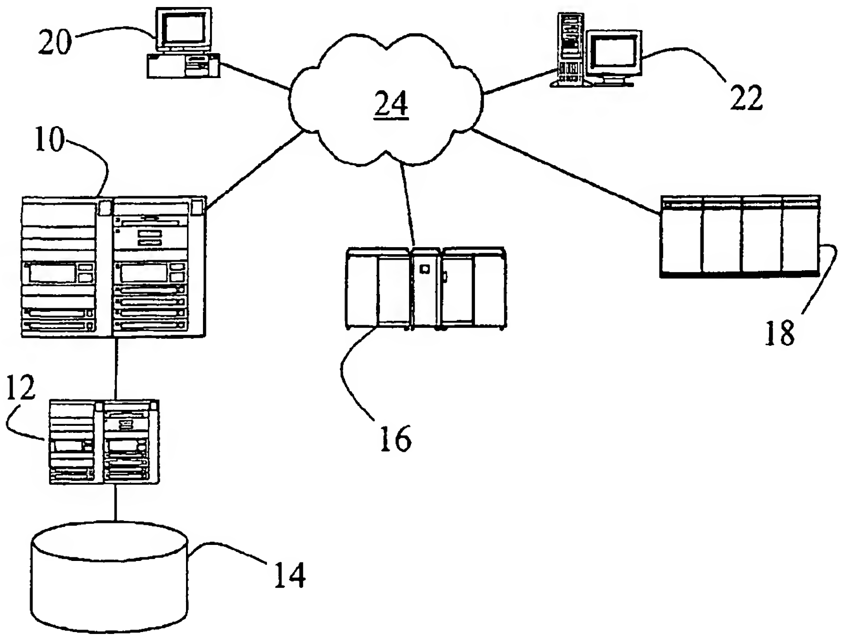
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TRANSACTION SYSTEM AND METHOD



(57) Abstract: The present invention provides a system and method for authenticating a financial transaction on an on-line network, the method involving: receiving a transaction request from a purchaser including unique information relating to the purchaser; authenticating the transaction request, and if authenticated, providing the purchaser with a transaction number, different from the purchaser's credit/debit card number, which the purchaser uses in order to effect the financial transaction.

TRANSACTION SYSTEM AND METHOD

TECHNICAL FIELD

The present invention relates to a system and/or method in the field of commercial transactions and notably to the field of electronic transactions in an on-line environment. The present invention has particular application to Internet banking and e-commerce operating systems.

BACKGROUND ART

With the advent of on-line networks, such as the Internet, commercial transactions in an on-line environment have become increasingly prevalent. Innumerable on-line sites now exist offering users a multitude of products and services that may be purchased via electronic transactions.

In undertaking on-line transactions, there is a general demand by users for such transactions to maintain their anonymity and privacy, as well as the assurance that personal financial information is not being compromised, particularly in relation to the disclosure of credit card numbers and their associated expiry date information.

For example, users wanting to purchase goods and services from a particular site are usually required to submit their credit or payment card details to the merchant. A problem with this approach is that the merchant is then availed of the user's credit details, so that the possibility exists for the merchant to misuse the details. For example, should a person's credit card number and related expiry date be obtained by a disreputable person, such as an errant merchant or computer hacker, then that person could use the number and date to make purchases on-line without the consent of the true owner of the card.

Credit card fraud is a particular problem for merchants, as most credit providers have a "card not present" policy whereby on-line merchants are held responsible for all fraudulent transactions. Therefore many on-line merchants suffer significant losses in revenue due to this policy.

From the users' point of view, when their credit card number is stolen, the credit provider deactivates the number and a new account installed. This process is time consuming, costly and generally disruptive for the account holder, as the existing credit card number cannot be used for any further transactions once the number is deactivated.

One previous attempt to solve the security problem has been Secure Electronic Transaction (SET) Technology. This technology requires a credit card to be authenticated via a smart chip reader installed on the user's computer system before the impending transaction. It is an on-line equivalent of presenting a credit card to a merchant to approve a transaction. While this technology is considered to provide a reasonably secure form of on-line transaction authentication, since the installation of a specialised card reader is required, the user's secure use of their credit card is restricted, as they are unable to purchase goods and services from other computer systems without such a reader installed.

In addition, there has been a general reluctance from users to accept the use of such specialised hardware for on-line transactions.

Another approach has been the authentication of the user via digital certificates that are first encrypted and then authenticated by the on-line merchant. A limitation of this technology is that there is to-date no single industry-wide standard for these certificates, so the user may end up with various types of different digital certificates to be used with various merchants. In addition, the system may be abused by disreputable merchants who misuse such certificates for unauthorized transactions.

There is therefore a need for a transaction system and/or method that provides users with an improved degree of anonymity, privacy and/or security.

The present invention seeks to overcome or alleviate at least one of the problems of the prior art.

SUMMARY OF THE INVENTION

According to a first aspect the present invention provides a method of authenticating a financial transaction between a purchaser and a merchant on an on-line network, including the steps of receiving a transaction request from a purchaser including unique information relating to the purchaser; authenticating the transaction request, and if authenticated, providing the purchaser with a transaction number, different from the purchaser's credit/debit card number, which the purchaser uses in order to effect the financial transaction.

It will be understood, however, that "purchaser" may include any user wishing to effect a payment, and that "merchant" may include any party to whom the purchaser wishes to make that payment. The payment could of course be for a good or a service, but it might also be intended to settle an existing debt, such as by paying a bill, so that a past purchase is settled, constitute an advance payment, or even merely to effect funds transfer between accounts. It will also be appreciated by those in the art that the transaction number (which may also be referred to as a "mutant number", "mutant account number", "mutant payment number" or "mutant card number", referring to its generally being different each time it is used) need not have any relationship with the purchaser's "genuine" credit/debit card or account number, or indeed that such a "genuine" credit/debit card number exists. It is envisaged that a credit account, for example, could be operated exclusively by the method (or system below) of the present invention, and that the transaction numbers, typically generated as required, could be the only numbers used to access that account. Further, the transaction number need not be generated from, or modified from, the purchaser's credit/debit card number.

Preferably the merchant uses the transaction number to complete the financial transaction with the purchaser's credit provider.

Preferably the method includes generating said transaction number from a password or phrase supplied by said purchaser. More preferably the method includes generating a pool of transaction numbers from a password or phrase supplied by said purchaser, and selecting said transaction number from said pool of transaction numbers.

According to a second aspect, the present invention provides a system for enabling a financial transaction in an on-line environment between a purchaser and a merchant, the system including purchaser authenticating means adapted to receive unique user identification information from the purchaser and to authenticate the purchaser based on the data and transaction number generator adapted to generate a transaction number, used by the purchaser in effecting the financial transaction the transaction number being different from the purchaser's credit/debit card number.

Preferably the transaction number is randomly generated and is generated for sole use in the transaction being authorised. This is because the transaction number is regenerated for each transaction, and therefore changes per transaction.

Therefore, by having a credit card number that is generated by the credit provider upon request for authorization by the purchaser, a secure and private transaction may be undertaken. In other words, the merchant is not availed of private credit details that may be subject to misuse.

Accordingly, an advantage of this invention is that a purchaser need not submit a fixed credit card number to any merchant.

According to another aspect, the present invention provides a method of authenticating a financial transaction between a purchaser and a merchant on an on-line network, wherein the purchaser is requesting the transaction from a mobile telephone with a SIM card, including the step of:

authenticating the purchaser's credit via the SIM card and/or a unique PIN.

According to a further aspect, the present invention provides a method of authenticating a financial transaction between a purchaser and a merchant, said method involving:

receiving a request from a purchaser for a transaction number, said request including identification information relating to said purchaser; and

authenticating said request, and if authenticated, providing the purchaser with said transaction number for use by said purchaser in effecting the financial transaction.

According to a still further aspect, the present invention provides a method for a purchaser to effect a financial transaction with a merchant, said method involving:

said purchaser submitting a request for a transaction number, said request including identification information relating to said purchaser;

said purchaser receiving said transaction number if said request has been authenticated; and

providing said transaction number to said merchant in order to effect the financial transaction.

According to another aspect, the present invention provides a system for enabling a financial transaction between a purchaser and a merchant, said system having:

purchaser authenticating means operable to receive from said purchaser a request for a transaction number, said request including identification information, and to authenticate said purchaser based on said identification information; and

a transaction number generator operable to generate a transaction number associated with said purchaser for use by said purchaser in effecting said financial transaction.

The system is of particular application in on-line environments (such as over the internet, including WAP by means of a WAP enabled telephone, short messaging service (SMS) or any other telephony data protocol), but could also be used in effecting transactions over the telephone or even in person. The important feature is that the transaction number is generated or given to the purchaser upon request - typically just before it is needed. Thus, the transaction number could be obtained by telephone, and then used over the telephone or in person as would any conventional credit card number.

Preferably said transaction number is different from a credit/debit account or card number of said purchaser.

Thus, it is preferable that the purchaser can always provide a number that is different from the "genuine" number associated with the credit/debit account being used (that is, the number that would otherwise be used, especially when making a face-to-face transaction) so that that number is not then provided to the merchant and held on the merchant's server. Merchants' servers are of unknown and often poor security. Even if all merchants' servers were secure, it is undesirable that copies of the purchaser's "genuine" number be present on potentially many servers of such merchants.

In one embodiment, the transaction number may include at least a portion of a genuine account or card number of said purchaser.

Alternatively, the transaction number may include at least a portion of a common account or card number of said purchaser. Preferably said common account or card number is specific to a particular financial institution, or a particular merchant.

Preferably said transaction number is selected from an existing set of such transaction numbers, preferably according to either a predetermined selection code or a selection code generated as needed

Preferably said set of transaction numbers is specific at any time to a single user.

In another embodiment, when said request is submitted from a device with a display (such as a computer screen), said identification information includes one or more hotspots, each hotspot located at a respective predetermined location adjacent to a character of said identification information. Preferably each of said hotspots is input by double clicking at said respective predetermined location or by leaving a cursor at said respective predetermined location.

Preferably the respective location of each hotspot is invisible after its entry.

In one embodiment, the identification information includes a previously provided answer to a corresponding question, whereby said method includes asking said purchaser said question and declining to authenticate said purchaser if said answer is not provided as a part of said identification information. The question and answer may be one of pluralities of such questions and corresponding answers.

In another embodiment, the method includes receiving said transaction number, modifying said transaction number by adding at least one hotspot to said transaction number, and providing said transaction number so modified to said merchant.

According to another aspect of the present invention, there is provided a method of effecting a financial transaction between a purchaser and a merchant, involving:

providing purchaser account information to said merchant;

said merchant requesting transaction approval from a credit issuer (or agent thereof);

said credit issuer sending an authentication request to said purchaser; and

said purchaser responding to said authentication request by sending authentication data to said credit issuer.

Preferably said authentication code comprises a reply to said authentication request.

Thus, if, for example, the authentication request is sent to the user's telephone (by WAP, email, SMS, etc), the user could simply use the reply function on his or her telephone to verify that the transaction is authenticate.

Alternatively, and for greater security, the authentication request could include a password (such as a PIN), which must be included by the user in the authentication data for the transaction to be authenticated.

Preferably said authentication data must include a predetermined password (such as a PIN) not included in said authentication request.

In one embodiment, the method includes sending said authentication data to said card issuer with said account information. For example, said account information could comprise a credit account number or a common credit issuer number; that number and the authentication data (which might be a PIN obtained by logging into the credit issuer's server) could be entered into the merchant's credit details console screen.

Preferably said method includes performing initial validity checks before sending said authentication request from said credit issuer to said purchaser.

Thus, the credit issuer might check, for example, if the account information is valid.

Preferably the authentication data comprises a requested portion or entirety of a password or phrase supplied by said purchaser.

In one embodiment, the authentication data comprises a predetermined first portion of a password or phrase supplied by said purchaser and a requested second portion of said password or phrase. The selection of the second portion can be changed at each log-in, preferably effectively randomly.

Preferably the first portion is delimited by a hotspot previously supplied with said password or phrase by said purchaser.

According to another aspect of the present invention, there is provided a method of effecting a financial transaction between a purchaser and a merchant, involving:

receiving a request for transaction approval from said merchant;

sending an authentication request to said purchaser; and

receiving authentication data from said purchaser.

In one aspect of the invention, there is provided a method of authenticating the identity of a user to a server in an on-line or other telecommunications environment, including the steps of:

establishing a user account with an associated user identification information and receiving, from said user, a password;

generating a pool of pseudo-passwords on the basis of said password and a code derived from said password;

receiving a log-in request from said user at a user device including said user identification information;

activating a pseudo-password from said pool of pseudo-passwords and generating a set of one or more numbers, wherein one of said set of numbers is derived from said code according to a rule;

transmitting to a user device said set of numbers;

entering said password into said user device and modifying said set of numbers according to said password and an inverse of said rule at said user device to produce a modified set of numbers;

transmitting said modified set of numbers to said server, said modified set of numbers including said code if said password has been entered correctly by said user;

releasing said selected pseudo-password and effecting user log-in if said modified set of numbers includes said code.

Preferably the password includes a hotspot with a position in or relative to said password.

Preferably the method includes locating said code in said set of numbers on the basis of said hotspot position.

Preferably the code is generated from a first hash value derived from said password independent of said position of said hotspot and a second hash value derived from said position of said hotspot.

Preferably the method includes generating said code by means of a session specific rule.

In a still further aspect of the present invention, there is provided a method of authenticating the identity of a user to a server in an on-line or other telecommunications environment, including the steps of:

receiving a log-in request from said user including unique information relating to said user;

authenticating the log-in request, and if authenticated, providing said user with a log-in number, which said user uses in order to log-in to said server.

BRIEF DESCRIPTION OF THE DRAWINGS

Illustrative embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 illustrates an example of an order form on a merchant's on-line site for use with a system for effecting financial transactions according to a first embodiment of the present invention;

Figure 2 illustrates an example of the type of billing information to be entered to place an order at a merchant's on-line site according to an embodiment of the invention;

Figure 3 illustrates an example of a window that may be presented to the user to provide a connection with a credit provider according to an embodiment of the invention;

Figure 4 illustrates the provision of a transaction number to a user for use in an on-line transaction according to an embodiment of the invention;

Figure 5 illustrates an example of the user using the transaction number on a merchant site to complete a transaction according to an embodiment of the present invention;

Figure 6 is a schematic representation of a system for effecting financial transactions according the first embodiment of the present invention;

Figure 7 is a schematic representation of a detail of the system of Figure 6 illustrating the manner in which user identify is established;

Figure 8 is a schematic representation of a detail of the system of Figure 6 illustrating the provision of a transaction number;

Figure 9 is a schematic representation of a detail of the system of Figure 6 illustrating the inclusion of the time of request of a transaction number in credit authorization;

Figure 10 is a schematic representation of a reserved list of transaction numbers in a system for effecting financial transactions according to a further embodiment of the present invention;

Figure 11 illustrates the manner in which access to the reserved list of Figure 10 is initiated;

Figure 12 illustrates the generation and use of a morph code to select a transaction number according to the further embodiment;

Figure 13 illustrates the transmission of the transaction number to a user according to the further embodiment;

Figure 14 illustrates the swapping of reserved lists of transaction numbers between users according to the further embodiment;

Figures 15A and 15B illustrate the insertion of hotspots into user identification information in a system for effecting financial transactions according to a further embodiment of the present invention;

Figure 16 illustrates the augmentation of user identification information with personal information in a system for effecting financial transactions according to a still further embodiment of the present invention; and

Figures 17A, 17B and 17C illustrate the augmentation of user identification information with personal information inserted in the password field in a system for effecting financial transactions according to a yet further embodiment of the present invention.

DETAILED DESCRIPTION

According to a first embodiment of the present invention, there is provided a system whereby electronic payment cards, such as credit cards are provided to a plurality of users, whereby the number appearing on the card is common to all such cards issued under the system. For present purposes, this number will be referred herein as the universal number. One or more suitable credit providers, such as a bank or other credit institution would issue these cards.

These cards are be individualized by virtue of an alternative identification means. For example, the user may have a unique user ID and/or password.

As an example of how such a payment/credit card would be utilised, a user wishing to make a purchase on-line would proceed to a particular merchant site. The user may access the site by any suitable means, such as a computer, mobile phone or any other network connected device. The user would then select products and/or services for purchase, such as by indicating the appropriate products/services on an order form, as illustrated in Figure 1, or placing the products/services in an electronic "shopping trolley". The merchant would await an indication from the user that they were proceeding with the transaction, such as by activating a "Buy" button or the like.

If the user has not already provided the merchant with general billing information, the merchant would request such information. For example, the user may be presented with a billing form as shown in Figure 2. In this regard, the number entered into the card or account number field is the universal number. It is to be appreciated that the universal number as used in Figure 2 is purely for the purposes of illustration of the invention, and that this number may be any number whatsoever. By entering the universal number, the user's privacy is maintained, as all users of this credit/debit system would share the same credit/debit card number, so that it is not possible to distinguish or differentiate the identity of the card owner by this number.

The merchant's site would recognise that the number submitted was the universal number. Preferably, a command would then be sent from the merchant's site to the user's browser to automatically launch a console program, which establishes a secure connection between the user and the credit provider's system and also causes the console screen as shown in Figure 3, to be presented to the user.

Alternatively, however, the console program need not be automatic, and the user may manually initiate this program, either from within their browser (in the case of a plug-in program) or by launching a stand-alone program.

The overlying console screen or window of the console program provides a graphical interface for the user to communicate with an authentication server. This authentication server is preferably independent from the one or more credit providers. In other words, a third party may control the authentication server, and the associated credit authorisation, for one or more credit providers. Alternatively, the authentication server is under the direct control of the credit provider.

In this regard, according to the present embodiment of the invention, the user would enter their unique information, such as a user name and password. This communication between the user and the authenticating server is a secured connection, so that the merchant is not able to access the user name or the password.

Once the authentication server receives the unique information from the user it verifies that information in the usual manner. If the authentication is positive, a single use transaction number is generated to be used in the transaction between the purchaser and the merchant. This transaction number may be randomly generated or retrieved from a predetermined list of numbers. For each successive authentication performed by the authentication server, a new transaction number is generated. It is preferably generated by the authentication server, although it may be generated by any other means or server associated with the authentication server. It is also to be appreciated that the transaction number is described as single use, in that it is generated to be used only once. In other words, it is not intended to mean that once a particular number is generated it is never regenerated again. It is possible for the same number to be regenerated and used in a different transaction.

Preferably the transaction number is sent from the authentication server to the user, as illustrated in Figure 4. The user would use this transaction number in the impending transaction, such as by modifying or replacing the number in the "card or account number" field as illustrated in Figure 5. Preferably, however, the console program automatically places the transaction number in the "card or account field" for the user's ease of use. To then place the order, the user could activate the "Yes: Place Order" field.

The transaction number preferably comprises two components: the first series of digits identify the bank or card issuer, while the last series of digits constitute a transaction number unique to the current transaction. For example, a transaction number "4569 4093 6011 0523" could comprise bank code "4569 4093 6" and transaction number "011 0523".

The merchant would then process the credit card transaction as usual by submitting the transaction details, including the transaction number, for approval. Preferably the authentication server provides this approval or another server associated therewith. Therefore, where the third party is controlling the authentication server, it is the third party's authenticating system that signals to the merchant's server whether the transaction is approved or rejected.

An overview of the architecture of the system of the first embodiment, and its operation, is illustrated schematically in Figures 6 to 9. Referring to Figure 6, the system includes a payment gateway 10, which includes an authentication server 12 with a user ID and password database 14, a credit authentication system 16 and the card issuer host system 18. The user's computer 20 and the merchant's server 22 communicate with each other and with the system of this embodiment by means of the internet 24.

Communications between the user's computer 20 and the merchant's server 22 are SSL (Secure Sockets Layer) data encrypted transmissions. Those between the merchant's server 22 and the payment gateway 10 (for authorization & data capture) are SSLv3 authenticated, encrypted transmissions. Transmissions between the payment gateway 10, the authentication system 16 and the card issuer host system 18 comprise authorization/data capture transmissions.

Referring to Figure 7, the order form 26 (similar to that of Figure 1) is presented by merchant server 22 to user computer 20. As described above, when the user provides the universal number and that number is identified as such by the merchant server 22, the merchant server 22 launches a console program 28, which prompts the user to enter user name and password information. That information is sent as an SSL data encrypted transmission 30 via the payment gateway 10 to the authentication server 12. Referring to Figure 8, if the user name and password details provided by the user are genuine, the authentication server 12 authenticates the user's ID and accesses the user's account details 32. The authentication server 12 then generates a transaction number 34 and sends the transaction number by SSL data encrypted transmission 36 to user computer 20.

As described in the context of Figures 4 and 5, the user then inserts the received transaction number in the order form 26. The order form is sent to the merchant's server 22 and from there to the credit authentication server 16 for authorisation, by means of an SSLv3 encrypted transmission. Referring to Figure 9, if the credit request is authorised by credit authentication server 16, credit authentication server 16 sends a credit authorisation 38 as an SSLv3 authenticated, encrypted transmission 40 to payment gateway 10. The payment gateway 10 then forwards the credit authorisation 38 to the merchant server 22.

Importantly, however, the credit authorisation 38 includes a "time issued" field 42, that is, the time at which the transaction number was issued. In this embodiment, before forwarding the credit authorisation 38 to merchant server 22, the payment gateway 10 compares the time the transaction number was issued with the time the payment gateway 10 received the credit authorisation 38. Only if the difference between these two times is less than a preset maximum will the credit authorisation 38 be passed on to the merchant server 22. Thus adds a level security, as a transaction number effectively expires if not used promptly. Consequently, the transaction number is preferably both one-use and valid for a finite time only, but either of these security measures is also of value.

Therefore, it is apparent that the present invention has the ability to make use of a user's credit card account without revealing or compromising the information relating to the user's real credit information, ensuring on-line privacy from both the merchant and potential hackers of the merchant's site. In particular, it is possible for a user to remain anonymous while making a transaction. Further, should a hacker gain access to the merchant's server and to transaction information stored on that server (should it be stored there), the information would be useless, as it would consist of transaction numbers which would not be able to be re-used.

The present invention also provides operational robustness and ease of administration, as a single credit card number makes it simple and effective for the card issuer to manage and administer a large number of users. Also, where the authentication is via a user ID and password, there is no need for any form of digital certificate to authenticate the transaction, which reduces costs and workload. Further, the authentication information is readily altered by the user and/or credit provider, which also aids the ease of use of the system.

An additional feature of the present invention relates to the provision of a transaction slip or confirmation to the user for each transaction that is authorised. This transaction slip is preferably provided to the user via one or more pre-selected address, such as an email address and/or wireless access protocol (WAP) mobile phone browser, SMS or any other network connected address. This transaction slip would be essentially a confirmation of the transaction that was generated.

This "transaction slip" is a counter check, and is not referred to during the user's authentication process, so the fraudulent user would not know at which email account the real user would be notified. Therefore, should a fraudulent transaction take place, the real user would be notified via email of the unauthorised transaction, and hence be able to take action.

An additional preferred feature, to further ensure that the user's identity is not revealed to the merchant, is for the user to request delivery to be provided to a prearranged location, such as a particular shop or café that is convenient for the user. Such an arrangement would require the assistance of the particular shop or café in order to be viable.

Alternatively, the user could enter a "virtual address" either to distinguish him or herself from other users, or to distinguish one of his or her orders from other orders he or she places. A virtual address may or may not be a real address, as its principal function is to specify identity, not location. This is done by entering the virtual address together with a unique PIN (Personal Identification Number) or other code, separated from the virtual address by a suitable ASCII separator character, such as the "&" symbol. This character serves as a separator so that both the virtual address and PIN (or equivalent) can be entered into the same input field. Alternatively, if all addresses are uniform in some way (e.g. never end in a numeral) and so are the PINs (e.g. comprise numerals exclusively), the system will be able to distinguish the virtual address from the PIN and the separator can be omitted.

For example, therefore, if the virtual address were "34 Moon Avenue, The Moon" and the PIN were "1234", in this embodiment the user would enter when prompted "34 Moon Avenue, The Moon&1234".

Vendors such as couriers, cafes or even selected or trusted merchants might provide the use of such common addresses to the purchasers (i.e. the users) for a small fee/charge per use. All users of such a payment card would then use the same virtual address; each user would be distinguished on the basis of his or her distinct PIN. The central server will recognise the various different common virtual addresses that, say, a courier company might provide, and route delivery to the courier company's server for processing. The courier company's server will then look for the "&" separated PIN, compare that PIN against a stored database where the real address of the courier's client (the ultimate purchaser or user) is found, and thus making the subsequent delivery from the merchant's warehouse to the purchaser's real address.

According to another embodiment of the present invention, the credit card may also be used offline. In this embodiment of the invention, the card has another unique Offline Credit Card (OEC) Number. This OEC number may be stored on the magnetic strip of the card and/or a smart chip embedded on the card. The credit card owner can make user of the card offline, while being fully assured that the OEC number, even if it were revealed, could not be used for any on-line transactions. Separate authenticating networks for on-line and offline transactions ensure that the OEC number could not be used for any on-line transactions, effectively making it usable only for "card present" transactions.

In this embodiment of the invention, each on-line and OEC transaction would be registered and the details submitted to the user's specified address, such as an email account, mobile phone WAP address or SMS. This empowers the user with complete information on all transactions made, whether on-line or offline so that they may deactivate or activate their on-line and/or offline accounts as required.

As indicated earlier, the present invention may be over a WAP enabled mobile telephone or by SMS. In a first embodiment, the user would input a user ID and/or PIN via the phone, in the same manner as indicated above. Once verified, the user would receive a transaction number on the mobile phone browser to be provided to the merchant to complete the transaction.

An alternative embodiment of the invention, implemented on a WAP enabled mobile phone with a SIM card will now be described. To obtain authorization for a particular transaction, a secure connection is established between the user's phone and a SIM Card authentication server. A third party preferably controls this server under licence from one or more credit providers, although the credit provider may alternatively control it. The credit provider may also be the user's telecommunications service provider.

At this site, the user is authenticated via their SIM card. For even greater security, the user may be authenticated using their SIM card as well as a PIN input by the user. If the authentication is positive, then a transaction number is generated. This transaction number may be sent to the user via the secure connection for completing the transaction with the merchant in the manner indicated in the previous embodiment.

Alternatively, instead of the transaction number being provided to the user, it may be maintained on the authentication server (or another server associated therewith) and is related with the merchant's order form once it is received by the authentication server. The transaction would then be authorised by the authentication server, if applicable. The merchant is then preferably sent the transaction number to hold as the credit card number for the transaction, and also a transaction slip may be sent to the user via their pre-selected email and/or mobile phone address. It is also to be appreciated that this alternative verification process may be applied to the previous embodiments of the invention herein described. Variations and additions are possible within the general inventive concept as will be apparent to those skilled in the art.

For example, instead of the console screen appearing, according to another embodiment of the invention, a link may be provided to the user to the credit provider's server or another server controlled by the user's credit provider in order to complete the authorisation at that site.

Also, on-line merchants may themselves provide the universal payment cards of the present invention.

Further, the obtaining of unique information from the user need not occur by the user entering their user name and password. For example, the authentication may be initiated without user input, such as by the automatic detection of some unique feature that the authentication server might process in the form of installed hardware/software.

In addition, it is possible to have more than one universal number, but such that a plurality of users still use each universal number. For example, a plurality of different credit providers may utilise the present invention and each credit provider may have their own universal number that they provide to their customers.

Referring to Figure 10, according to another embodiment of the present invention, the transaction number is provided to the user/purchaser in a two step process. The authentication server 12 maintains, for each user/purchaser 42, a list 44 of already generated possible transaction numbers in a database reserved for this purpose. Referring to Figure 11, the user 42 enters the required unique identification information (that is, a user name and password) in console screen 28 and clicks "OK" to send that information to the authentication server 12. Referring to Figure 12, the authentication server 12 responds - assuming that the ID information was valid - by providing or generating a selection or "morph" code 46 comprising an alphanumeric string, in this example "&jd(fkwse@2)". The morph code 46 is then used by authentication server 12 to select which of the transaction numbers in the reserved list 44 is to be used (in this example transaction number 48). This selection can be by any suitable method; a checksum could be generated from the morph code, the value of which specifies the entry in the reserved list of transaction numbers to be used. Alternatively, the morph code 46 could be used as a random number generator seed, the resulting random number specifying which entry in the reserved list of transaction numbers to be used.

Alternatively, rather than relying on a reserved list of available transaction numbers, the morph code 46 could be added to the universal (or common) number based on ascii values of each character to yield the transaction number.

Referring to Figure 13, the transaction number 48 so specified is then "activated", that is, recorded as valid for use by user 42, and sent 50 either to the user (for subsequent submission to the merchant) where it is displayed in window 52, or directly to the merchant (not shown), as described in the above embodiments.

After the transaction is completed, the activated transaction number 48 is deactivated and thus rendered useless.

At any subsequent log-on, the authentication server 12 ensures that the issued morph code is different from any morph code to that user previously, to randomise the transaction number selected for each transaction.

Referring to Figure 14, furthermore the reserved number database for each user is also periodically interchanged with that of another user, enabling the cardholder's submitted transaction number to be truly single-use, disposable and secure for each transaction. Thus, the reserved list 44 of user 42 could be swapped with the reserved list 54 of user 56 so that user 42 has reserved list 54 and user 56 reserved list 44; alternatively, in typical system with many users, the reserved lists can periodically be randomly re-assigned amongst the users.

As a further layer of security in any of the above embodiments, the required unique identification information (that is, the user name and password) to be sent by the user to the authentication server may include one or more "hotspots". Each hotspot in inserted into the user name or the password by double clicking at the desired location, next to any of the characters of the user name or password. Such hotspots would not generally be recorded by the user with user name/password details and, indeed, according to the invention need not be visible on the computer screen. They are, however, agreed upon - in much the same manner as the user name and password - by the user and credit provider.

Referring to Figure 15A, the user name 58 and password 60 are first entered in the conventional manner in the console screen 28 provided - at the prompting of the authentication server 12 or merchant server 22 - for this purpose. Referring to Figure 15B, the user then double clicks at a number of predetermined locations (in this example after the eighth character of both the user name 58 and the password 60), to insert hotspots. Each hotspot can be regarded, in fact, as a part of the respective user name or password. In the illustrated example, the locations of the hotspots are shown by means of the "|" character; however, it may be preferred that no visible character be displayed after the hotspots have been entered.

Such hotspots can also be added to the transaction number itself. The transaction number will typically be received by the user in a pop-up window or console. The user can then copy the transaction number and paste it into the on-line ordering console provided by the merchant server. Before doing so (or after doing so but before selecting the "OK" button on the merchant's order form), the user can insert one or more hotspots into the transaction number by double clicking at predetermined locations (previously arranged with the credit provider). In this embodiment, without these hotspots the transaction number is incomplete and invalid.

Optionally, in addition to the usual user name and password (with or without hotspot(s)), the user can be asked a question at each log-on, at regular intervals, or when the authentication server 12 detects abnormal log-on time or log-on behaviour. This so-called "question of the day" acts, in effect, as a second level password in addition to the user name and password. The user's personal particulars, such as age, address, or even information that is specifically designed for the above purposes, such as most memorable moment, favorite car make, etc. can be selected to become answers to "question of the day" passwords. During the initial user registration (to register or first log-on to the authentication server/party), the user is asked a series of questions and informed that the answers will constitute "question of the day" log-on fields in addition to the user's user name/password information.

These questions are then rotated to accompany the username and password that the user must input to log-in, so that the user is asked a different "question of the day" at regular log-on attempts.

Rotation of this "question of the day" effectively increases the level of security associated with log-on authentication via keyboard or keypad devices.

Thus, referring to Figure 16, at log-in to the authentication server 12, the user is presented with a log-in console screen 62 containing the usual fields 64 and 66 for user name and password respectively.

In addition, console screen 62 includes a "question of the day" 68, to which the user must respond by inserting the correct answer in field 70 before selecting the "OK" button 72. Only if both the password and this answer are correct for the user name will the user be logged into the authentication server 12 and provided with a transaction number (as described above).

In one alternative approach, the answer to the "question of the day" is entered by the user following and in the same field as the password. Thus, referring to Figure 17A, the user is again presented with a login console screen 74, which contains input fields 76 and 78 for user name and password (with or without hotspot(s)) respectively. The console screen 74 also includes a "question of the day" 80. As shown in this figure, the user enters his or her user name and password in fields 76 and 78 in the usual manner.

Referring to Figure 17B, as soon as the password has been entered, a field separator 82 is preferably inserted after the password in the password field 78. This field separator 82 is preferably automatically inserted by the authentication server 12 as soon as the correct number of password characters (nine in the illustrated example) are detected, whether or not the password has been correctly spelt.

Referring to Figure 17C, the user then enters the answer 84 to the "question of the day" 80 immediately after the field separator 82; the user continues typing the answer 84 directly after the password has been entered as though the answer 84 were merely an extension of the password. The answer 84 is masked in the same manner as the password. In the illustrated example, the answer 84 so entered could read, for example, "21061965", such as might be the required answer if the "question of the day" 80 were "What is your Date of Birth? [ddmmyyyy]". After the user has entered the required answer 84, the user selects the "OK" button 86 to complete logging on. As in the approach described with reference to Figure 16, the "question of the day" 80 is regularly rotated, and is based on information obtained from the user during initial user registration.

In another alternative approach similar to that described above by reference to Figures 15A and 15B, identification also requires a password with a hotspot (where both password and hotspot are supplied initially by the user), but the password and hotspot are not stored by the system, on the authentication server or otherwise. Rather, in this approach the system initially generates and stores two "hash" values (the first from the password and the second from the hotspot position) and a large pool of pseudo-passwords (from both the password and hotspot position) for later use. This is done when the user's account is established and preferably on the authentication server. Any suitable rules or algorithms may be used do generate these hash values and pseudo-passwords.

The rule or rules used to select the pseudo-password for activation from the pseudo-password pool can be adapted from any suitable existing algorithms such as MD5 from RSA Security. However, since a large library of different rules or algorithms can be used to determine which pseudo-password pool is to be selected, hacking to determine the rule or algorithm is made much more difficult.

Thus, for example, a user might enter the password/hotspot "ace|3" (where the "|" character represents the location of the hotspot), on the basis of which the system could generate a first hash value of 10,000 from the password, a second hash value of 4 from the hotspot position, and the pool of pseudo-passwords:

- Password1
- Password1o2ijr
- Erpji335
- Erpfgopj
- 567-095346pas
- Thisispassword
- The brown fox234

None of these pseudo-passwords is - initially - activated, and none is ever valid as a password that can be entered by a user when prompted for a password at log-in.

When the user attempts to log-in, he or she first enters the appropriate user ID in the log-in dialog box user name field (say, for example, "ace_sing").

When the user tabs to the password input field in the log-in dialog box, the user ID is transmitted to the authentication server. The authentication server responds by selecting and activating one of the pool of pseudo-passwords, and by generating two numbers from the first hash value, the first number X to be stored on the authentication server, the second number Y to be sent to the user client device/terminal. X and Y are generated by means of two separate rules or algorithms, which are themselves session specific. A library of such algorithms will be cycled through effectively randomly so that the relationship between password via the first hash value to X and Y is more difficult to predict. In addition, as a result X and Y will almost certainly differ from previous X and Y values at each log-in session.

In this example and for this specific session, the algorithms might be:

X = (first hash value) × 2 / 4 and

Y = (first hash value) × 2 / 8,

so that, again in this example where the first hash value is 10,000, X = 5,000 and Y = 2,500.

The authentication server then determines a third value that reflects a relationship Z between the values of X and Y. In the simplest case, this might be merely the difference between X and Y. Thus in this example, Z = X - Y = 2,500.

A further algorithm is used to compute a factor R from this Z value, and Z is then modified according to R, preferably either by reducing or increasing Z by the value of R. Suppose, therefore, that an algorithm is used in this example that produces an R value of 32.55 from a Z of 2,500. If, in this case, Z′ equals Z minus R, Z′ = 2,500 - 32.55 = 2,467.45.

Until now the system has used only the first hash value in the generation of X, Y, Z, R and Z′. Now, however, the system uses the second hash value (from the hotspot position) to determine the correct place where the Z′ value should be in a sequence of numbers, to represent the 5 possible hotspots in the password, ace3 (i.e. "|ace3", "a|ce3", "ac|e3", "ace|3" and "ace3|"). With another algorithm or algorithms, the server generates from the value of Z four (i.e. one less than the number of possible positions) numbers, using another algorithm or set of algorithms, that are close to and within a pre-determined maximum deviation from Z. These might be, in this example where Z = 2,500:

2,670 2,355 2,493 Reserved 2,841

The second hash value (4 in this example) determines where the system places Z′ in the "reserved" position in this number sequence.

This number sequence is then transmitted to the client device (e.g. the user computer), while the user inputs into his or her computer the original password and hotspot. If the hotspot is inserted correctly, all the numbers in the number sequence:

2,670 2,355 2,493 2,467.45 2,841

are increased or decreased (in this embodiment increased) by the R value, 32.55, thereby creating the modified number sequence:

2,702.55 2,387.55 2,525.55 2,500 2,873.55.

That is, if Z was decreased by R to produce Z′, the number sequence should be increased by R to produce the modified number sequence (and *vice versa*).

The modified number sequence is transmitted to the authentication server, extracts the number (viz. 2,500) located at the position in the modified number sequence indicated by the second hash value (viz. 4), and compares that number with the value of Z (either stored or re-generated from X and Y).

The values of R and Z′ were selected in this example for clarity; in actual operation, the values of Z′ and R would preferably be generated such that the number sequence does not show a recognisable pattern (though all the numbers would still be increased or decreased by the same R value to obtain the modified number sequence to be transmitted back to the authentication server).

Importantly, since the number sequence that represents the possible hotspots in the password (five in the example of the password "ace3") are always different, and the numbers themselves deviate little from one another in value, it is difficult to derive the real position of the hotspot via tapping into the system and inspecting the number sequence. Thus, a hacker cannot gain access into the system even if in possession of the first and second hash values.

When the authentication server detects a match between Z and the number in the reserved position in the modified number sequence, the selected pseudo-password is released, the user is authenticated and log-in proceeds.

Thus, the user need not remember to change passwords, since – from the user's point of view - a single password can be used. However, the hotspot position might be changed periodically for added security.

In this approach, therefore, the system has three fail-safe mechanisms:

i) System access is not dependent on a single password, but from a large pool of pseudo-passwords;

ii) Selection of a single pseudo-password from such a pseudo-password pool can be determined by any suitable algorithm, so the relationship between the initial password and hotspot, and the ultimate pseudo-password from the pool on any particular log-in would be essentially unpredictable by a third party; and

iii) Optionally, although the user's hotspot position is preferably the same at each log-in, the numbers or characters representing that hotspot position could be changed at each log-in so that the hotspot position cannot easily be deciphered.

In another, similar approach, the user-provided password is treated by the system as comprising two portions. This can either be done at a hotspot specified by the user, or at a location dictated by the system. If dictated by the system, the location of the division can be fixed (e.g. after the nth character or such that the second portion comprises m characters), or specified and possibly varied each time the user is prompted for the password. For example, therefore, a user might provide the password "PASSWORD123" and be informed by the system (or specify by means of a hotspot) that the password will be divided such that the second portion comprises four characters, viz. "D123". These last four characters may be described, therefore, as "cut-away" from the password overall.

When the system prompts the user for the password, he or she is required to enter only the first portion, i.e.

the password without the cut-away portion or, in this example, "PASSWOR".

The system - preferably only if the correct first portion has been entered - then prompts the user for information concerning the second or cut-away portion. The requested information might be, for example, the entire second portion (in this example "D123"), a particular character - such as the third character - of the second portion (in this example "2"), or some other combination of the characters of the second portion.

Preferably the system inserts a password dot (comparable to field separator 82 shown in Figure 17B) immediately after the user has correctly entered the first portion, before then prompting for the desired information concerning the second portion.

In another approach, instead of the answer to a "question of the day" or a password, the user is prompted to enter a "Passphrase". The Passphrase is preferably initially supplied by the user, such as when the account is established. Each time the user attempts to log-in, the system requests either that the user enter the entire Passphrase (as though it were a password), or a specified portion or portions of the Passphrase. For example, if the Passphrase were "this is my passphrase", and the user were prompted for the third word of the Passphrase, the user would have to enter "my" to establish his or her identity.

Optionally, the system could designate a particular portion of the Passphrase to be entered initially at each log-in, display a password dot after that portion has been entered correctly, and prompt the user for one or more other portions of the Passphrase as described above.

According to a still further embodiment of the present invention, a user uses a WAP or SMS enabled mobile phone together with a personal credit or debit card and discloses his or her personal credit (payment) card number to merchant, irrespective of where the user conducts the financial transaction (be it a physical store, on the

Internet or otherwise). In the case of a WAP telephone, upon receiving the credit authorization request, the credit issuer server causes the iWAPGS server to send an alert to the user's WAP mobile phone of the impending transaction, to which the user replies by sending a (preferably prearranged PIN) authentication code that verifies (and authenticates) to the card issuer that the transaction is indeed effected by the user (and not some other party), so that the card issuer's server can complete the transaction. Only if the authentication code is submitted will the card issuer approve the transaction. Once the transaction has been completed, the user receives a second iWAPGS transaction notification that informs the cardholder of the details of the completed transaction information.

In effect, the user's credit card number is useless in both Internet and card-present transactions until the user submits the authentication code via a WAP mobile phone. This system can potentially reduce card-present card fraud (which is very much higher than web-based card fraud) from fraudulent practices such as card skimming. This WAP payment card system can also be implemented for use with the "morph code" approach described above.

The iWAPGS server transaction system can also be adapted for similar, transaction-based computer processes, such as when a computer user attempts log-in onto a certain computer server/network. When the user attempts to log-in using a User ID and password, the targeted server can also send (via the iWAPGS server) an alert to the user's mobile phone, where the user can simply reply via SMS or WAP protocol with a "Yes" or "No" confirmation, or a prearranged verification PIN number, confirming or disavowing the attempted access to the server.

Only when the user replies with a valid confirmation answer via the correct mobile telephone would the iWAPGS server grant the user access to the computer server/network to which the user is attempting log-in. This approach is similar to the iWAPGS server waiting for a confirmation reply from the user (in that case, purchaser) via a mobile telephone prior to the authentication and clearance for payment for the common/universal payment card system.

According to another embodiment of the present invention, the user sends a universal or common number (discussed above) as the payment number to the merchant, for the purpose of effecting a financial transaction. However, prior to the submission of such a common payment number, the user first logs onto a web server for authentication (by the card issuer). A common number submitted without the user's first logging onto - and gaining authentication from - the card issuer server is completely useless for any transaction. Via authentication, the card issuer will issue a transaction PIN number, that is only valid for one transaction and is discarded after the transaction is completed. This transaction PIN number is (preferably automatically) placed in any (predetermined) one of the existing data fields other than the payment or credit card number data field on the merchant's online purchase form (or any other electronic form that requires the user to submit information, such as payment number, shipping address etc.). The user (or preferably the user's electronic wallet program) could, for example, enter the PIN number in the "Name" field, and rely on the PIN number to identify the user.

Where the PIN number is automatically placed in a predetermined one of the existing data fields, the PIN number would be separated with a ASCII symbol such as "&" (or any other appropriate symbol) to allow the card issuing server to correctly identify the PIN from the existing data field, such as the "Name" field. This allows the user to submit (after authentication with the card issuing server/web-site) a common credit card number to the merchant, when in fact the card issuing server would have placed an unique, single-use transaction number and/or PIN within one of the data fields normally required by the purchaser to input on the merchant's shopping cart and/or online purchase form, separated by a "&" ASCII symbol.

Thus, the user uses the common payment number, and after authentication of his or her identity through logging on, instructs the card issuing server to issue another transaction PIN for use with the common number submitted to the merchant for that transaction. The common number AND the transaction PIN number (which is in reality encapsulated together within a pre-selected data in the online form) is then used for the authentication of the impending transaction.

The common number may consist of a running series of numbers assigned for a group of cardholders that might belong to a similar geographical location, country, or some other common similarity. Use of the common number provides the cardholder with the benefits of not having to disclose any personal financial information, and so be anonymous when making purchases online.

Thus, users can share a common payment card number, yet each user is still correctly distinguished and his or her transactions authenticated and approved.

Modifications within the spirit and scope of the invention may readily be effected by persons skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method of authenticating a financial transaction between a purchaser and a merchant on an on-line network, including the steps of:

receiving a transaction request from a purchaser including unique information relating to the purchaser;

authenticating the transaction request, and if authenticated, providing the purchaser with a transaction number, different from the purchaser's credit/debit card number, which the purchaser uses in order to effect the financial transaction.

2. A method as claimed in claim 1, wherein the merchant uses the transaction number to complete the financial transaction with the purchaser's credit provider.

3. A method as claimed in either claim 1 or 2, wherein the transaction number may only be used for a single transaction.

4. A method as claimed in claim 3, wherein the transaction number is randomly generated.

5. A method as claimed in any one of claims 1 to 4, wherein the purchaser initiates the transaction request from a mobile phone.

6. A method as claimed in claim 5, wherein the unique information relating to the purchase is obtained via the mobile phone's SIM card and/or a PIN entered by the purchaser.

7. A method as claimed in any one of claims 1 to 6, further including the step of:

generating a transaction confirmation to be sent to the owner of the credit/debit card via one or more prearranged network-connected addresses, such as an email address.

8. A system for enabling a financial transaction in an on-line environment between a purchaser and a merchant, the system including:

purchaser authenticating means adapted to receive unique user identification information from the purchaser and to authenticate the purchaser based on the data;

transaction number generator adapted to generate a transaction number used by the purchaser in effecting the financial transaction, the transaction number being different from the purchaser's credit/debit card number.

9. A system as claimed in claim 8, further including financial transaction authenticating means adapted to receive the transaction number from the merchant and to effect a further transaction between the merchant and the purchaser's credit provider.

10. A system for undertaking financial transactions in an on-line environment, including:

a plurality of credit cards, such that the cards physically have the same credit card number;

an authentication server for authenticating purchases to be made using the cards, such that the server:

authenticates unique information, provided by users of the cards, which is not physically associated with the cards; and

for a positive authentication, providing a user with a transaction number to be provided to a merchant as a credit card number, such that the transaction number is different to the physical credit card number.

11. A system as claimed in either claim 8 or 10, wherein the transaction number is randomly generated and only able to be used for a single transaction.

12. A system as claimed in either claim 8 or 10, further including a transaction confirmation generating means for generating a transaction confirmation to be sent to the owner of the credit/debit card via one or more prearranged network-connected addresses, such as an email address.

13. A system as claimed in either claim 10 or 11, wherein the plurality of credit cards include an off-line credit card number that may only be used for off-line credit transactions.

14. A system as claimed in claim 13, wherein the off-line credit card number is stored on a magnetic strip and/or a chip embedded on the card.

15. A system as claimed in either claim 13 or 14, wherein the credit card has separate credit accounts for on-line transactions and off-line transactions.

16. A method of authenticating a financial transaction between a purchaser and a merchant on an on-line network, wherein the purchaser is requesting the transaction from a mobile telephone with a SIM card, including the step of:

authenticating the purchaser's credit via the SIM card and/or a unique PIN.

17. A method of authenticating a financial transaction between a purchaser and a merchant, said method involving:

receiving a request from a purchaser for a transaction number, said request including identification information relating to said purchaser; and

authenticating said request, and if authenticated, providing the purchaser with said transaction number for use by said purchaser in effecting the financial transaction.

18. A method for a purchaser to effect a financial transaction with a merchant, said method involving:

said purchaser submitting a request for a transaction number, said request including identification information relating to said purchaser;

said purchaser receiving said transaction number if said request has been authenticated; and

providing said transaction number to said merchant in order to effect the financial transaction.

19. A method as claimed in any one of claims 16 to 18, wherein said transaction number includes at least a portion of a genuine account or card number of said purchaser.

20. A method as claimed in any one of claims 16 to 18, wherein said transaction number includes at least a portion of a common account or card number of said purchaser.

21. A method as claimed in claim 20, wherein said common account or card number is specific to a particular financial institution, or a particular merchant.

22. A system for enabling a financial transaction between a purchaser and a merchant, said system having:

purchaser authenticating means operable to receive from said purchaser a request for a transaction number, said request including identification information, and to authenticate said purchaser based on said identification information; and

a transaction number generator operable to generate said transaction number associated with said purchaser for use by said purchaser in effecting said financial transaction.

23. A system as claimed in claim 22, wherein said transaction number is different from a credit/debit account or card number of said purchaser.

24. A system as claimed in either claim 22 or 23, wherein said transaction number includes at least a portion of a genuine account or card number of said purchaser.

25. A system as claimed in either claim 22 or 23, wherein said transaction number includes at least a portion of a common account or card number of said purchaser.

26. A system as claimed in claim 25, wherein said common account or card number is specific to a particular financial institution, or a particular merchant.

27. A method of effecting a financial transaction between a purchaser and a merchant, involving:

providing purchaser account information to said merchant;

said merchant requesting transaction approval from a credit issuer or agent thereof;

said credit issuer sending an authentication request to said purchaser; and

said purchaser responding to said authentication request by sending authentication data to said credit issuer.

28. A method as claimed in claim 27, wherein said authentication code comprises a reply to said authentication request.

29. A method as claimed in claim 27, wherein said authentication request includes a password, which must be included by the user in the authentication data for the transaction to be authenticated.

30. A method as claimed in claim 27, wherein said authentication data must include a predetermined password not included in said authentication request.

31. A method as claimed in claim 27, including sending said authentication data to said card issuer with said account information.

32. A method as claimed in claim 27, including performing initial validity checks before sending said authentication request from said credit issuer to said purchaser.

33. A method of effecting a financial transaction between a purchaser and a merchant, involving:

receiving a request for transaction approval from said merchant;

sending an authentication request to said purchaser; and

receiving authentication data from said purchaser.

34. A method as claimed in any one of claims 1, 16, 17, 18, 27 or 33, including deactivating said transaction number after a predetermined time period, so that said transaction number is made unusable even if not yet used.

35. A method as claimed in any one of claims 1, 16, 17, 18, 27 or 33, wherein said transaction number is selected from an existing set of such transaction numbers.

36. A method as claimed in claim 35, wherein said transaction number is selected from said set of transaction numbers according to either a predetermined selection code or a selection code generated as needed.

37. A method as claimed in claim 35, wherein said set of transaction numbers is specific at any time to a single user.

38. A method as claimed in any one of claims 1, 17, 18, 27 or 33, wherein, when said request is submitted from a

device with a display, said identification information includes one or more hotspots, each hotspot located at a respective predetermined location adjacent to a character of said identification information.

39. A method as claimed in claim 38, wherein each of said hotspots is input by double clicking at said respective predetermined location or by leaving a cursor at said respective predetermined location.

40. A method as claimed in either claim 38 or 39, wherein the respective location of each hotspot is invisible after its entry.

41. A method as claimed in either claim 38 or 39, including receiving said transaction number, modifying said transaction number by adding at least one hotspot to said transaction number, and providing said transaction number so modified to said merchant.

42. A method as claimed in any one of claims 8, 17, 18 or 22, wherein said identification information includes a previously provided answer to a corresponding question, whereby said method includes asking said purchaser said question and declining to authenticate said purchaser if said answer is not provided as a part of said identification information.

43. A method as claimed in claim 42, wherein said question and said corresponding answer are one of pluralities of such questions and corresponding answers.

44. A system as claimed in any one of claims 8, 10 or 22, wherein said system is operable to deactivate said transaction number after a predetermined time period, so that said transaction number is made unusable even if not yet used.

45. A system as claimed in any one of claims 8, 16, 17 or 18, wherein said transaction number is selected from an existing set of such transaction numbers.

46. A system as claimed in claim 45, wherein said transaction number is selected from said set of transaction numbers according to either a predetermined selection code or a selection code generated as needed.

47. A system as claimed in claim 45, wherein said set of transaction numbers is specific at any time to a single user.

48. A method as claimed in any one of claims 1, 17, 18, 27 or 33, wherein said request includes address information and qualifying data, said address information indicative of said purchaser and said qualifying data indicative of a further party.

49. A method as claimed in claim 48, wherein said further party is a customer of said purchaser.

50. A method as claimed in either claim 48 or 49, wherein said address information is fictitious.

51. A method as claimed in either claim 48 or 49, wherein said address information corresponds to a real address.

52. A method as claimed in any one of claims 48 to 51, receiving said address information and said qualifying data are entered into the same input field.

53. A method as claimed in claim 52, including receiving said address information and said qualifying data separated by at least one character.

54. A method of authenticating the identity of a user to a server in an on-line or other telecommunications environment, including the steps of:

establishing a user account with an associated user identification information and receiving, from said user, a password;

generating a pool of pseudo-passwords on the basis of said password and a code derived from said password;

receiving a log-in request from said user at a user device including said user identification information;

activating a pseudo-password from said pool of pseudo-passwords and generating a set of one or more numbers, wherein one of said set of numbers is derived from said code according to a rule;

transmitting to a user device said set of numbers;

entering said password into said user device and modifying said set of numbers according to said password and an inverse of said rule at said user device to produce a modified set of numbers;

transmitting said modified set of numbers to said server, said modified set of numbers including said code if said password has been entered correctly by said user;

releasing said selected pseudo-password and effecting user log-in if said modified set of numbers includes said code.

55. A method as claimed in claim 54, wherein said password includes a hotspot with a position in or relative to said password.

56. A method as claimed in claim 55, including locating said code in said set of numbers on the basis of said hotspot position.

57. A method as claimed in either claim 55 or 56, wherein said code is generated from a first hash value derived from said password independent of said position of said hotspot

and a second hash value derived from said position of said hotspot.

58. A method as claimed in any one of claims 54 to 57, including generating said code by means of a session specific rule.

59. A method as claimed in either claim 27 or 33, wherein said authentication data comprises a requested portion or entirety of a password or phrase supplied by said purchaser.

60. A method as claimed in either claim 27 or 33, wherein said authentication data comprises a predetermined first portion of a password or phrase supplied by said purchaser and a requested second portion of said password or phrase.

61. A method as claimed in claim 60, wherein said first portion is delimited by a hotspot previously supplied with said password or phrase by said purchaser.

62. A method of authenticating the identity of a user to a server in an on-line or other telecommunications environment, including the steps of:

receiving a log-in request from said user including unique information relating to said user;

authenticating the log-in request, and if authenticated, providing said user with a log-in number, which said user uses in order to log-in to said server.

63. A method of authenticating the identity of a user to a server in an on-line or other telecommunications environment, including the steps of:

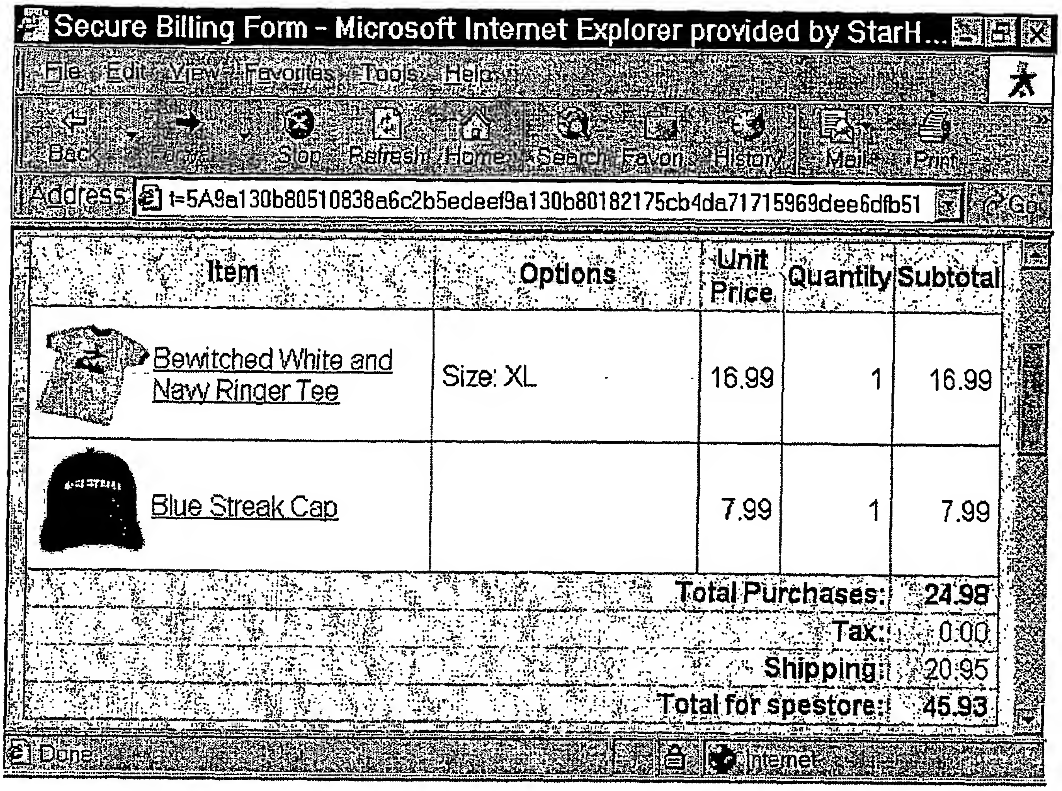
sending to a mobile telephone or other portable communications device of said user an authentication request;

deeming user identity verified if said user responds to said request by sending a suitable response from said mobile telephone or other portable communications device.

64. A method as claimed in claim 63, wherein said server sends said request and receives said response via a gateway corresponding to said mobile telephone or other portable communications device.

65. A method as claimed in claim 64, wherein said gateway is an iWAPGS server.

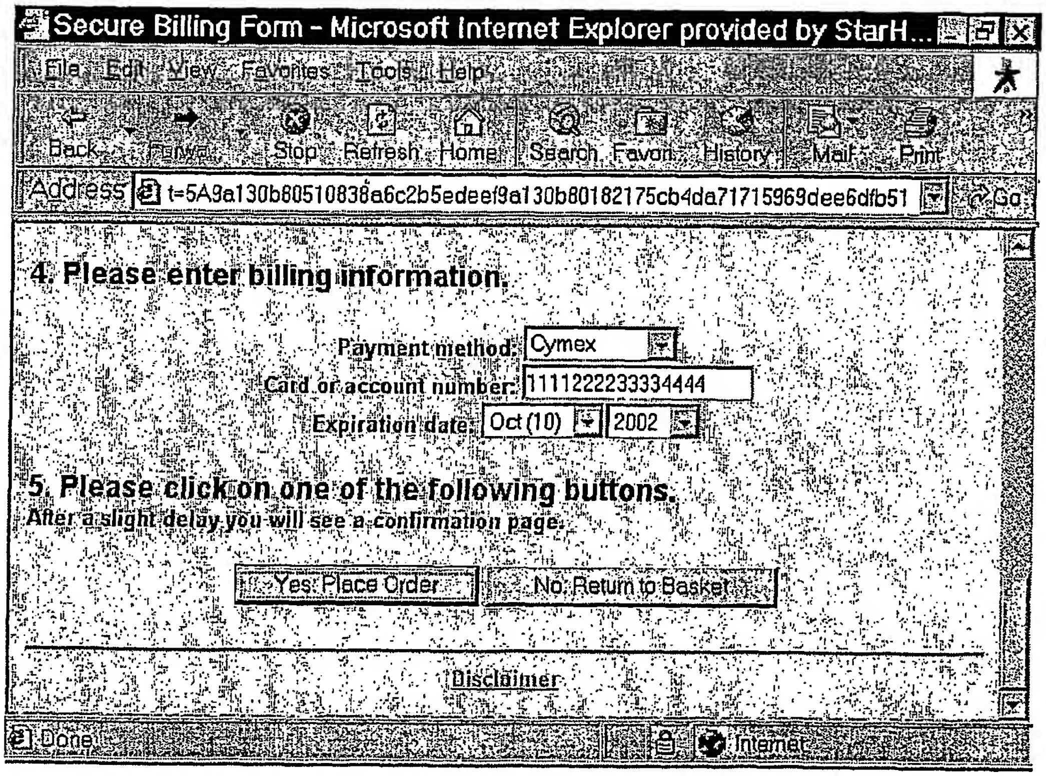
66. A method as claimed in any one of claims 63 to 65, including requiring that said response be received within a predetermined time after said request is sent and deeming any subsequent response to said request unsuitable.


Secure Billing Form - Microsoft Internet Explorer provided by StarH...
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address
Go
Done
Internet

Address: t=5A9a130b80510838a6c2b5edeef9a130b80182175cb4da71715969dee6dfb51

Item	Options	Unit Price	Quantity	Subtotal
Bewitched White and Navy Ringer Tee	Size: XL	16.99	1	16.99
Blue Streak Cap		7.99	1	7.99
			Total Purchases:	24.98
			Tax:	0.00
			Shipping:	20.95
			Total for spestore:	45.93

Figure 1



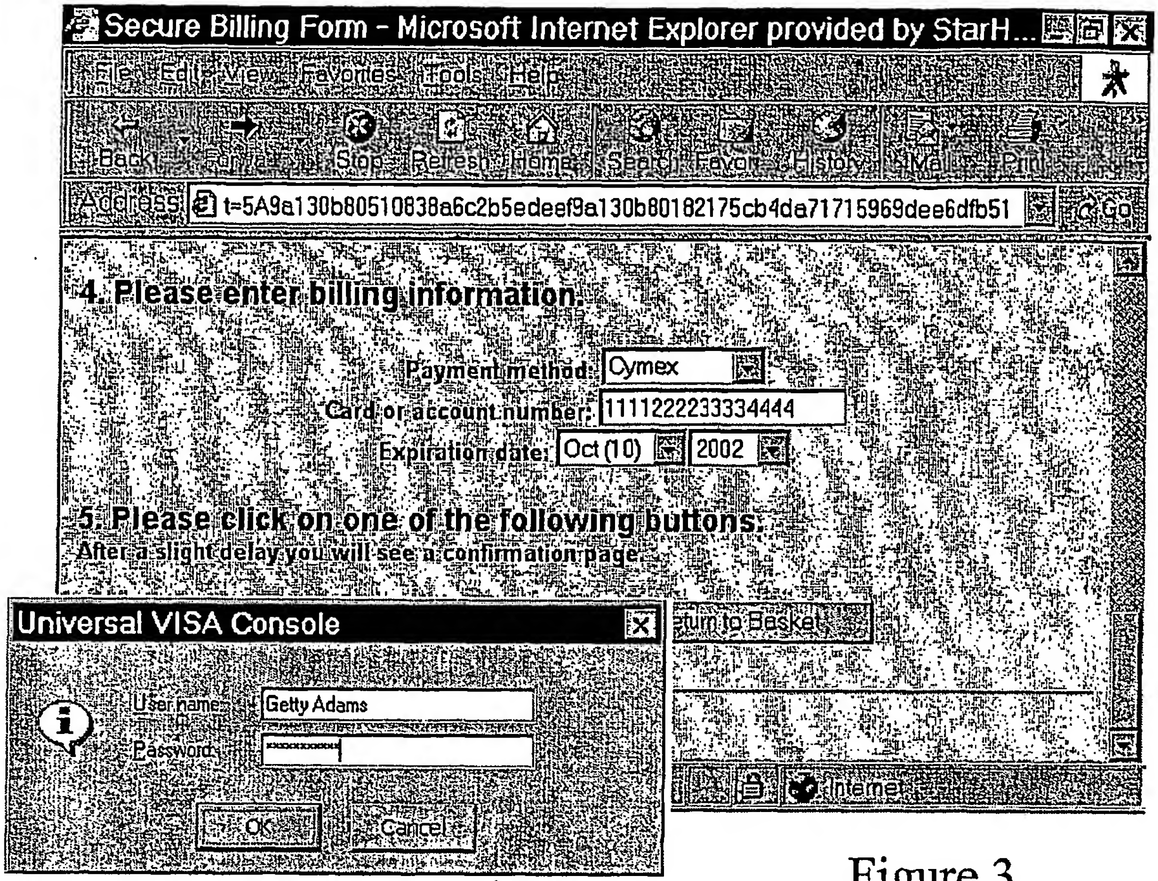
Address: t=5A9a130b60510838a6c2b5edeef9a130b80182175cb4da71715969dee6dfb51

4. Please enter billing information.

Payment method: Cymex
Card or account number: 1111222233334444
Expiration date: Oct (10) 2002

5. Please click on one of the following buttons.
After a slight delay you will see a confirmation page.

Figure 2


Secure Billing Form - Microsoft Internet Explorer provided by StarH...
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favori History Mail Print
Address
Go
Return to Basket
Internet
Universal VISA Console
OK
Cancel

Address: t=5A9a130b80510838a6c2b5edeef9a130b80182175cb4da71715969dee6dfb51

4. Please enter billing information.

Payment method: Cymex

Card or account number: 1111222233334444

Expiration date: Oct (10) 2002

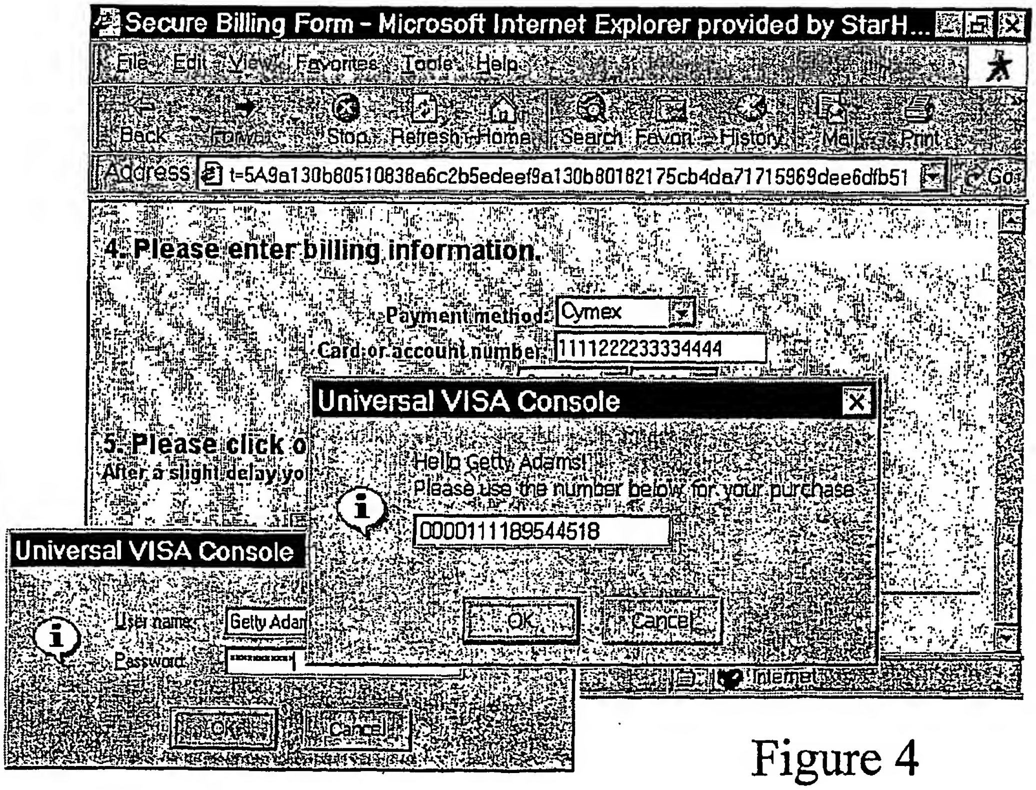
5. Please click on one of the following buttons.

After a slight delay you will see a confirmation page.

User name: Getty Adams

Password: **********

Figure 3


Secure Billing Form - Microsoft Internet Explorer provided by StarH...
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favori History Mail Print
Address
Go
Internet
Universal VISA Console
OK
Cancel
Universal VISA Console
OK
Cancel

Address: t=5A9a130b80510838a6c2b5edeef9a130b80182175cb4da71715969dee6dfb51

4. Please enter billing information.

Payment method: Cymex

Card or account number: 1111222233334444

5. Please click o

After a slight delay yo

Hello Getty Adams!

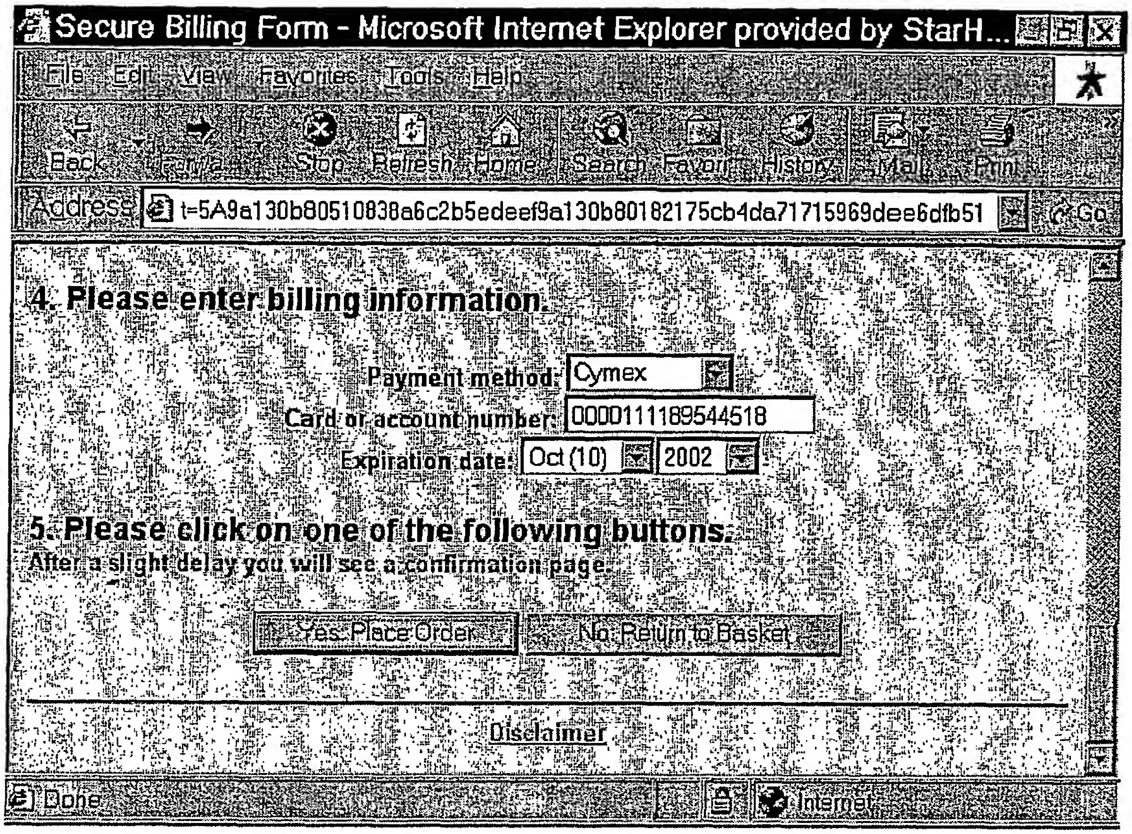
Please use the number below for your purchase

0000111189544518

User name: Getty Adan

Password: **********

Figure 4


Secure Billing Form - Microsoft Internet Explorer provided by StarH...
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address
Go
Yes, Place Order
No, Return to Basket
Disclaimer
Done
Internet

t=5A9a130b80510838a6c2b5edeef9a130b80182175cb4da71715969dee6dfb51

4. Please enter billing information.

Payment method: Cymex

Card or account number: 0000111189544518

Expiration date: Oct (10) 2002

5. Please click on one of the following buttons.

After a slight delay you will see a confirmation page.

Figure 5

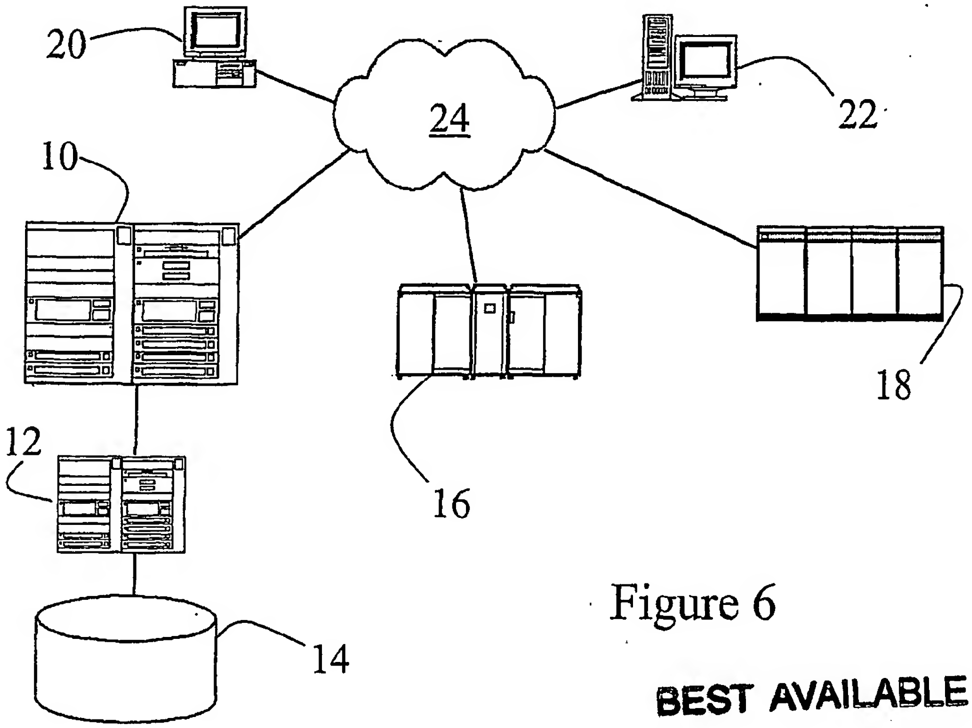
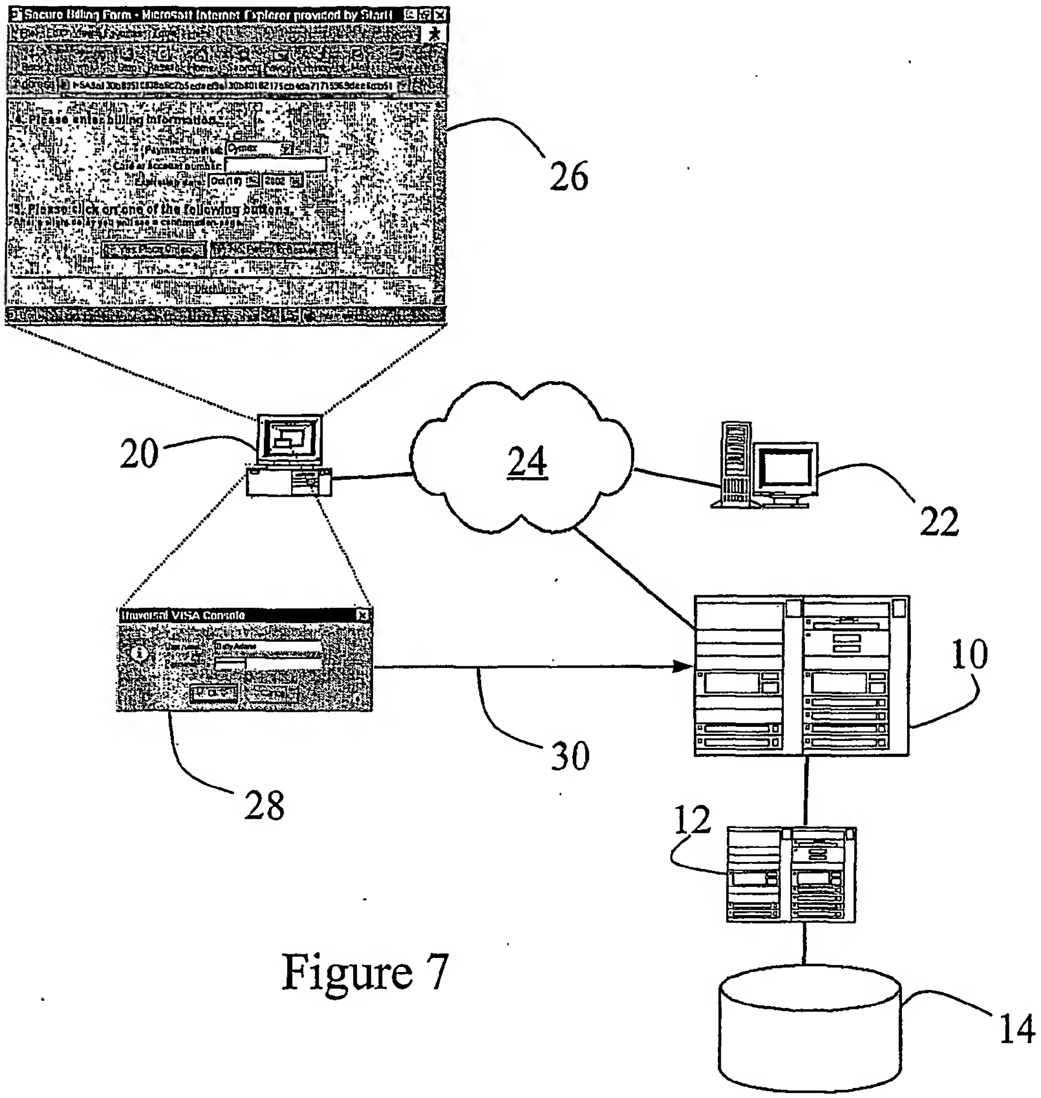


Figure 6



Secure Billing Form - Microsoft Internet Explorer provided by Start!

4. Please enter billing information.

Payment method: Cymex

Card or Account number:

Expiration date: Oct (10) 2002

5. Please click on one of the following buttons.

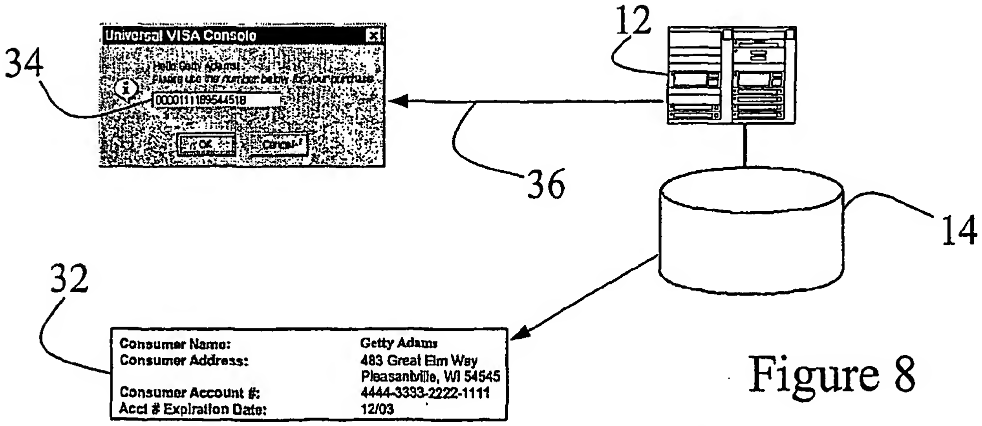
After a slight delay you will see a confirmation page.

Universal VISA Console

User name: Getty Adams

Password:

Figure 7



Universal VISA Console

Hello Getty Adams!

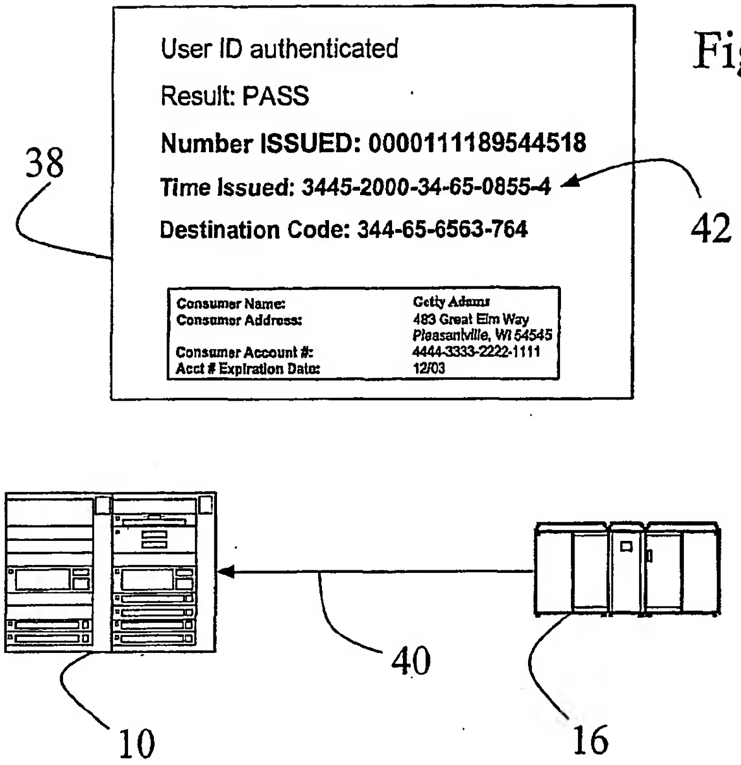
Please use the number below for your purchase.

0000111189544518

Consumer Name:	Getty Adams
Consumer Address:	483 Great Elm Way Pleasantville, WI 54545
Consumer Account #:	4444-3333-2222-1111
Acct # Expiration Date:	12/03

Figure 8

BEST AVAILABLE COPY



User ID authenticated

Result: PASS

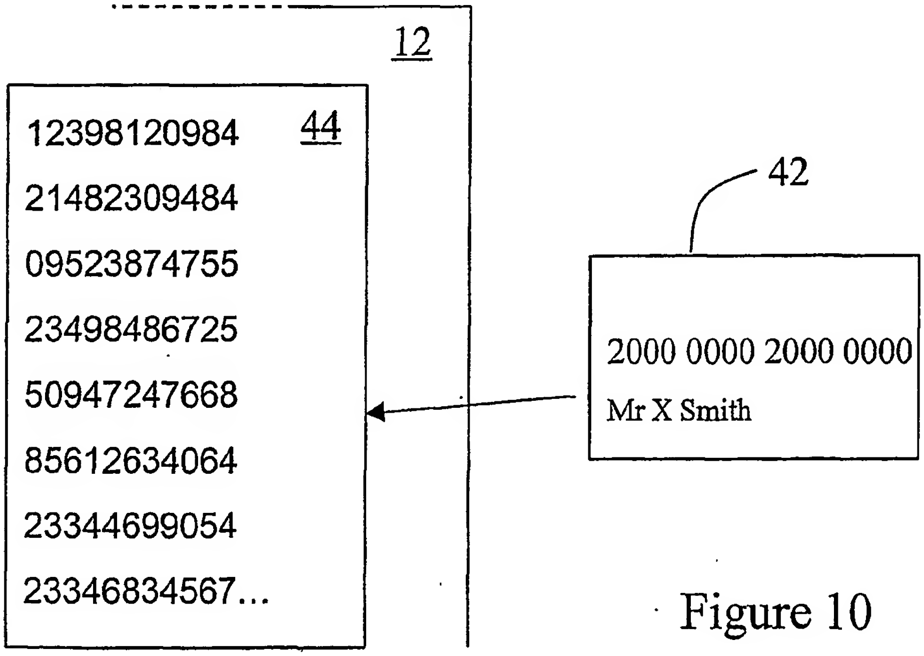
Number ISSUED: 0000111189544518

Time Issued: *3445-2000-34-65-0855-4*

Destination Code: 344-65-6563-764

Consumer Name:	**Getty Adams**
Consumer Address:	**483 Great Elm Way** ***Pleasantville, WI 54545***
Consumer Account #:	**4444-3333-2222-1111**
Acct # Expiration Date:	**12/03**

Figure 9



12398120984
21482309484
09523874755
23498486725
50947247668
85612634064
23344699054
23346834567...

2000 0000 2000 0000
Mr X Smith

Figure 10

Figure11

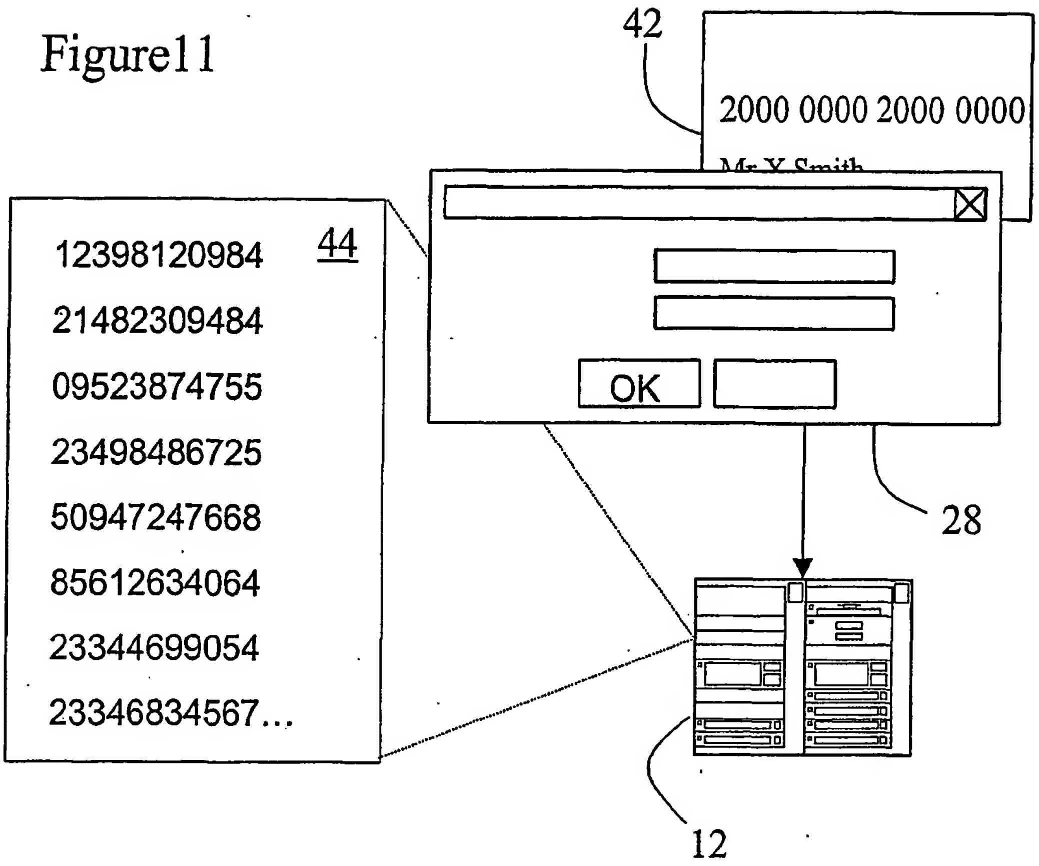
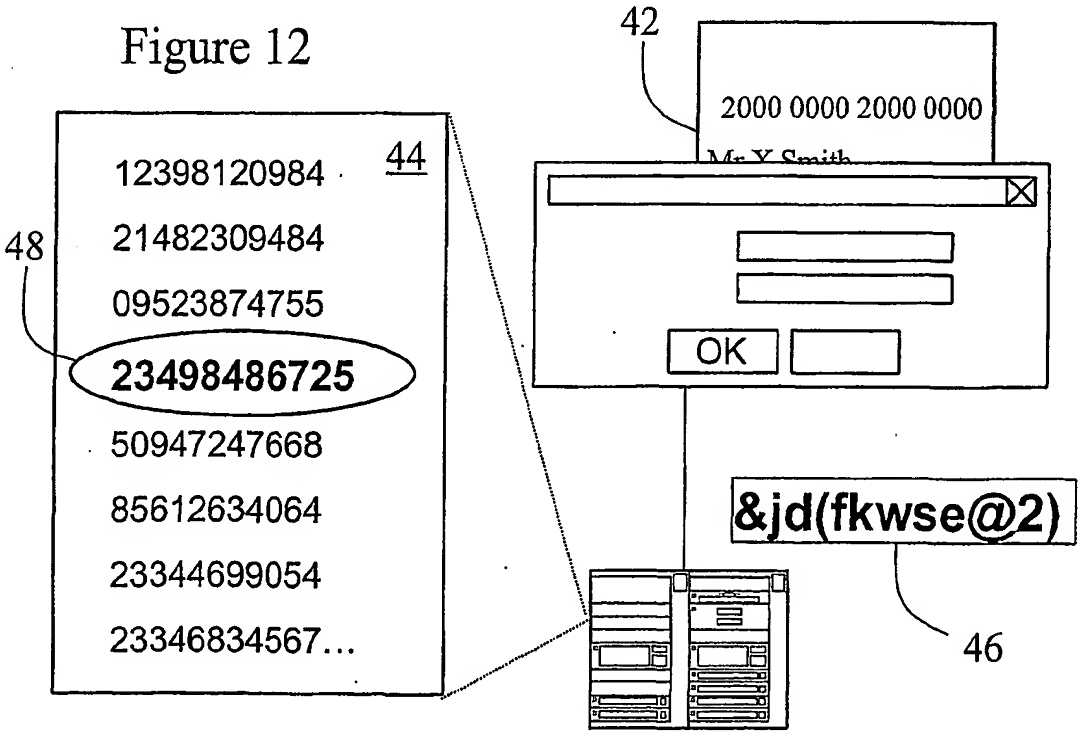


Figure 12



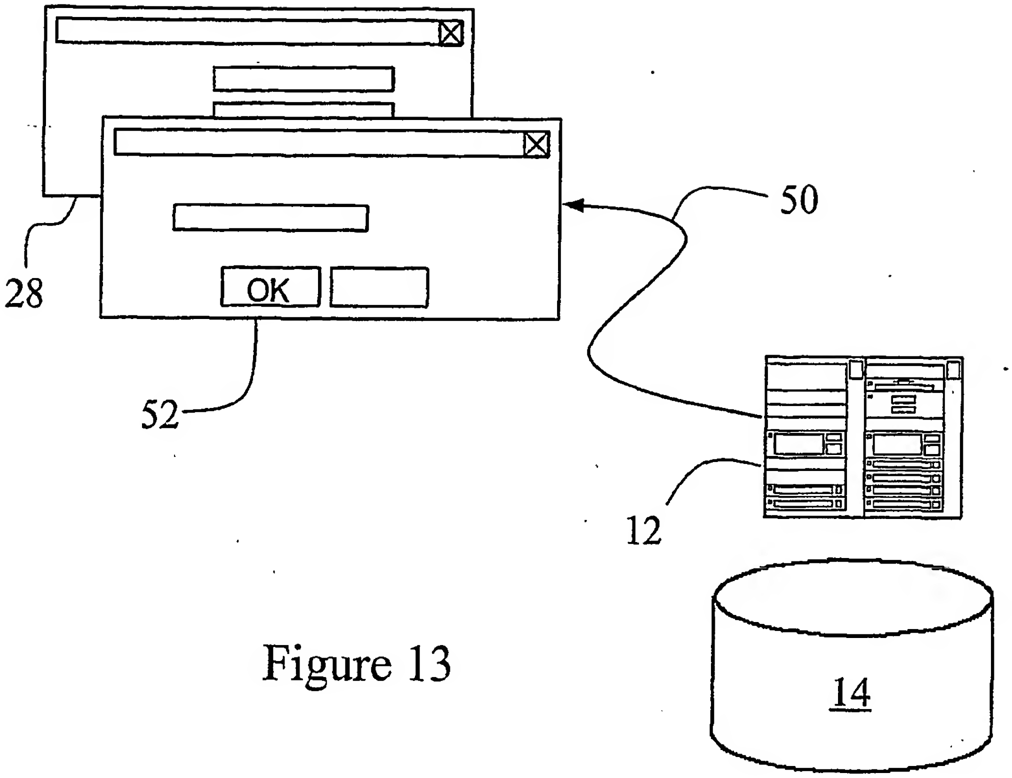


Figure 13

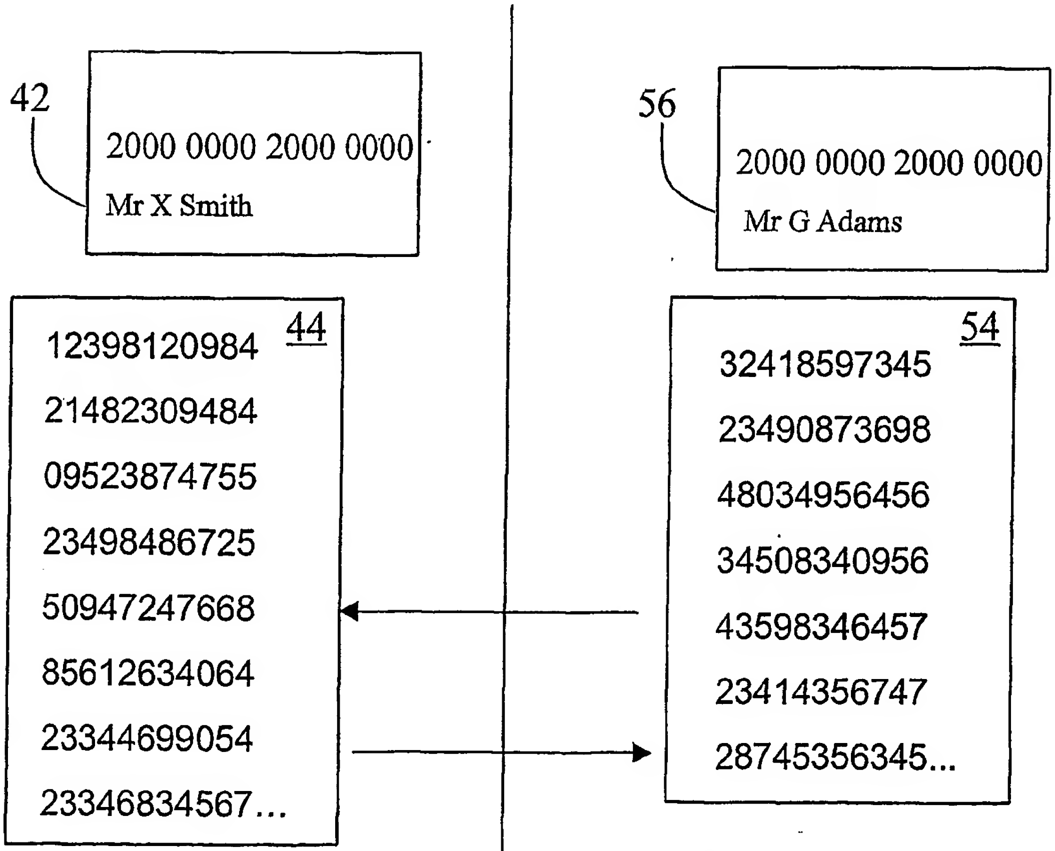
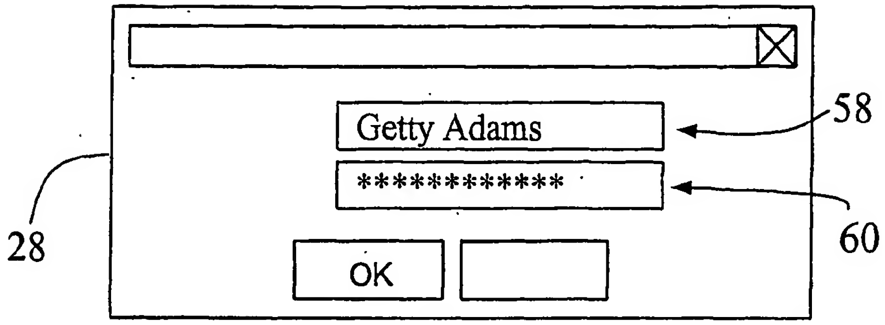
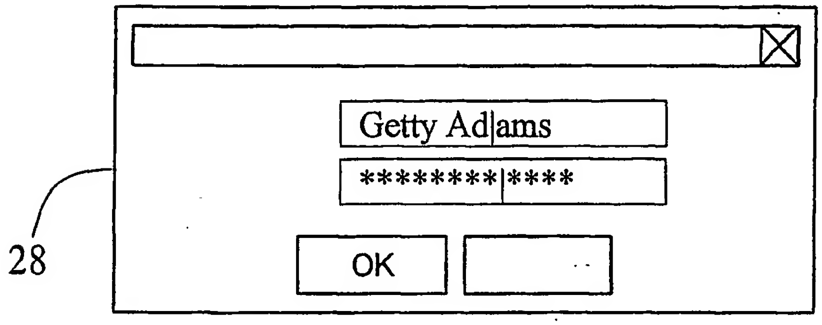


Figure 14


Getty Adams

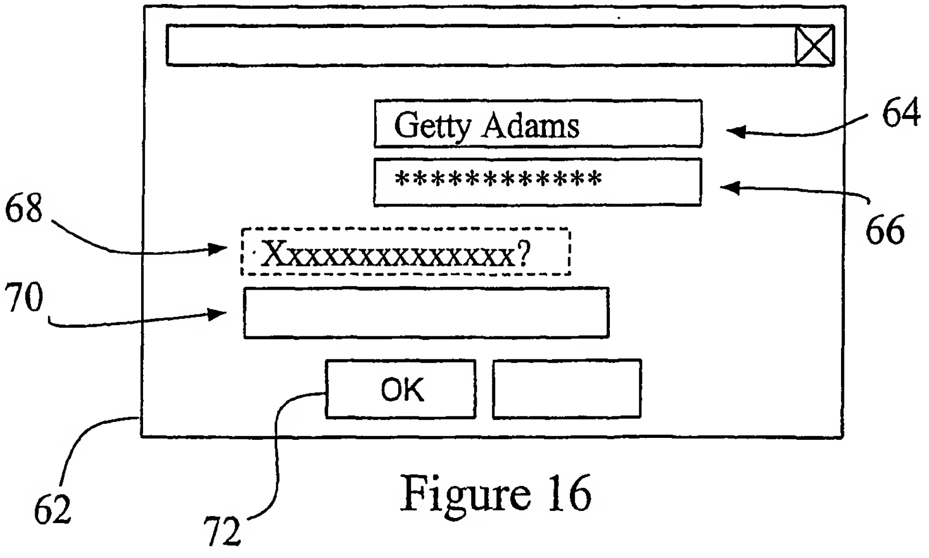
****

Figure 15A


Getty Ad|ams

********|****

Figure 15B


Getty Adams

****

Xxxxxxxxxxxxxx?

Figure 16

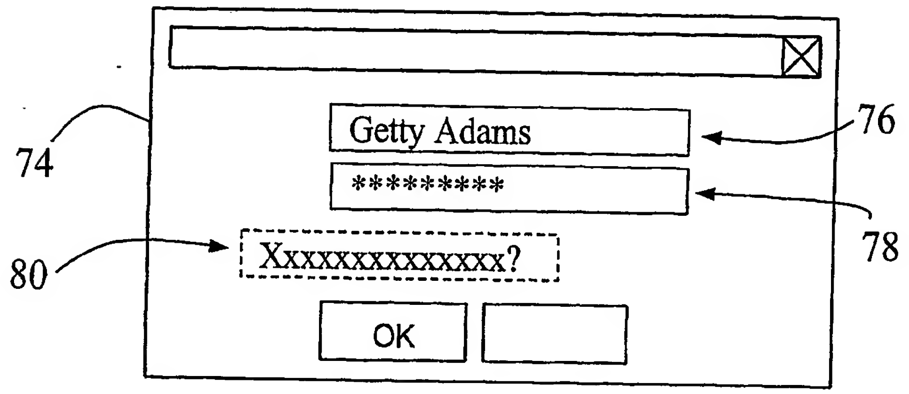


Figure 17A

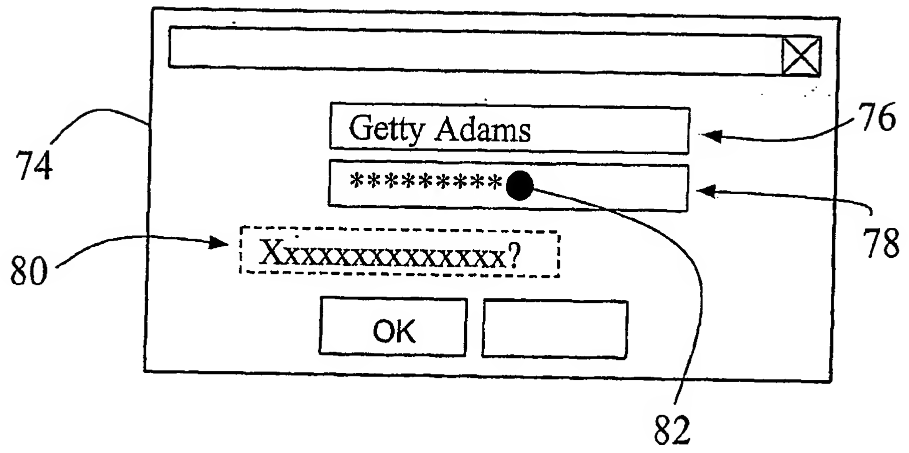


Figure 17B

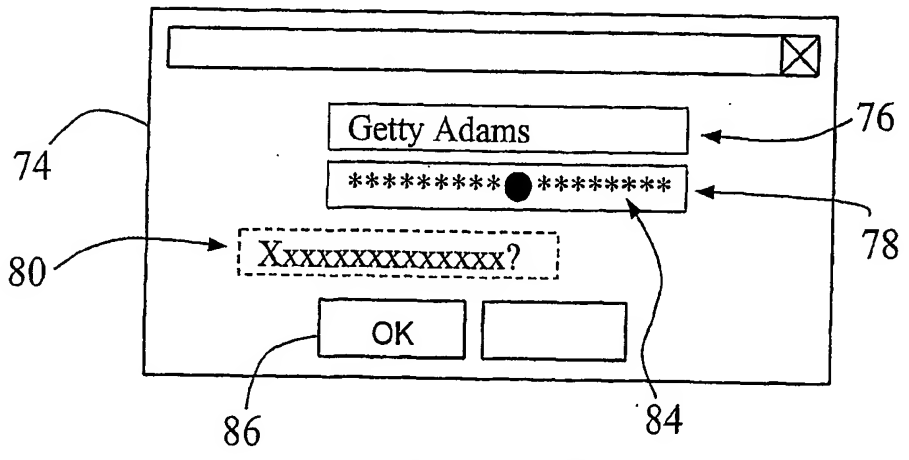


Figure 17C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG01/00102

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. ^{7}: G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT with keywords

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5883810 A (FRANKLIN et al) 16 March 1999	1 - 66
X	US 6000832 A (FRANKLIN et al) 14 December 1999	1 - 66
X	WO 99/49424 A (ORBIS PATENTS LIMITED) 30 September 1999	1 - 66

☒ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 19 September 2001	Date of mailing of the international search report 24 SEPTEMBER 2001
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer J.W. THOMSON Telephone No : (02) 6283 2214

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG01/00102

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	GB 2350982 A (PHILLIPPS) 13 December 2000	1 - 66
P,X	WO 00/79457 A (INTERNET REVENUE NETWORK, INC) 28 December 2000	1 - 66

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG01/00102

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5883810	NONE					
US	6000832	NONE					
WO	9949424	AU	30506/99	BR	9909065	EP	1029311
		EP	1115095	IE	990240	IL	137456
		NO	20004657				
GB	2350982	AU	200052328	WO	200077733		
WO	200079457	AU	200056262				

END OF ANNEX